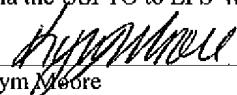


CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being transmitted via the USPTO to EFS-Web on September 6, 2006.


Kym Moore

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In Re Application of:

Date: September 6, 2006

Bruce BENFIELD, et al.

Confirmation No: 5418

Serial No: 09/734,403

Group Art Unit: 2131

Filed: March 8, 2001

Examiner: Aravind K. Moorthy

Title: METHOD AND SYSTEM FOR INTEGRATING ENCRYPTION
FUNCTIONALITY INTO A DATABASE SYSTEM

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

SUBSTITUTE BRIEF ON APPEAL

In response to the Office Communication mailed August 29, 2006, Appellant provides this Substitute Brief on Appeal including an "Evidence Appendix" and a "Related Proceedings Appendix" as set forth in 37 CFR 41.37.

(1) Real Party in Interest

The real party in interest is International Business Machines Corporation by virtue of an assignment from the inventors recorded in the U.S. Patent Office on July 9, 2001, reel no. 011972, frame no. 0873.

(2) Related Appeals and Interferences

There are no related appeals or interferences known to the Applicant.

(3) Status of Claims

Claims 1-5, 8-12, 15-18, 21-23 and 25-27 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,421,703 (“Steinmetz”).

Claims 6-7, 13-14, 19-20, 24 and 28 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Steinmetz in view of U.S. Patent No. 6,360,322 (“Grawrock”).

All of the foregoing claims are being appealed.

(4) Status of Amendments

There are no unentered amendments.

(5) Summary of Claimed Subject Matter

Independent claim 1 recites a method for integrating encryption functionality into a database system. The method includes providing at least two functions to support data encryption in a database system. Specification, page 5, lines 5–14. The method further includes utilizing the at least two functions within structured query language statements. Specification, page 5, line 18 – page 6, line 8.

Independent claim 8 recites a system for integrating encryption functionality into a database system. The system includes at least one computer processing device. Specification, page 4, lines 16-22; FIG. 1. The system further includes a database management system installed on the at least one computer processing device, in which the database management system supports utilization of at least two functions for data encryption. Specification, page 5, lines 1-7; FIG. 1. The at least two functions for data

encryption are invoked within structured query language statements. Specification, page 6, lines 4-8.

Independent claim 15 recites a computer readable medium containing program instructions for integrating encryption functionality into a database system. The computer readable medium contains program instructions for providing at least two functions to support data encryption in a database system. Specification, page 5, lines 5–14. The computer readable medium further contains program instructions for utilizing the at least two functions within structured query language statements. Specification, page 5, line 18 – page 6, line 8.

Independent claim 21 recites a method for integrating encryption functionality into a database system. The method includes defining a function to support encryption of data in a database system, in which the encryption of data is based on a user-specified password, and the function has a function name. Specification, page 5, lines 12-15; page 7, line 1. The method further includes utilizing the function within a structured query language statement to control access to the data in the database system including encrypting the data within the database system with the user-specified password. Specification, page 5, lines 18-23; page 6, lines 3-9. The structured query language statement includes the function name and the user-specified password. Specification, page 7, line 1.

Independent claim 25 recites a computer readable medium containing program instructions for integrating encryption functionality into a database system. The computer readable medium contains program instructions for defining a function to support encryption of data in a database system, in which the encryption of data is based on a

user-specified password, and the function has a function name. Specification, page 5, lines 12-15; page 7, line 1. The computer readable medium further contains program instructions for utilizing the function within a structured query language statement to control access to the data in the database system including encrypting the data within the database system with the user-specified password. Specification, page 5, lines 18-23; page 6, lines 3-9. The structured query language statement includes the function name and the user-specified password. Specification, page 7, line 1.

(6) Grounds of Rejection to be Reviewed on Appeal

1. Applicant requests review as to claims 1-5, 8-12, 15-18, 21-23 and 25-27 and their rejection under 35 U.S.C. § 102(e) as being anticipated by Steinmetz.

2. Applicant requests review as to claims 6-7, 13-14, 19-20, 24 and 28 and their rejection under 35 U.S.C. § 103(a) as being unpatentable over Steinmetz in view of Grawrock.

(7) Argument

1. **Claims 1-5, 8-12, 15-18, 21-23 and 25-27 are not properly rejected under 35 U.S.C. § 102(e) as being anticipated by Steinmetz.**

(A) Claims 1-5, 8-12, and 15-18

Claim 1 recites a method for integrating encryption functionality into a database system. In particular, the method includes providing at least two functions to support data encryption in a database system, and utilizing the at least two functions within structured query language statements (emphasis added).

Such a method has a potential advantage of providing a straightforward and flexible technique to protect confidential data in a database in a manner that allows

integration with well-established, non-proprietary SQL techniques (specification page 8, lines 3-10).

Steinmetz discloses a process and system for controlling the use of software – i.e., to prevent piracy of software programs (see Abstract; col. 1, ll. 26-29). Specifically, Steinmetz discloses utilizing a key – or an electronic device 7 – that is detectable by corresponding software program(s) during execution of the software program(s) (col. 1, ll. 42-46; FIG. 1). Codes can be read from or written to the key by calling upon a function (function cnrm) that is in the form of: result=cnrm(var1, var2, ... varn) with $n > 3$. The variables (var1 to varn) correspond to particular values associated with functions to be performed with the key (col. 2, ll. 10-32). These functions are listed in columns 9-10 of Steinmetz.

(A)(i) Steinmetz fails to disclose utilizing a function to support data encryption in a database system within a structured query language (SQL) statement.

The Examiner has rejected claim 1 based on Steinmetz's use of the "cnrm function". Steinmetz discloses, however, that the cnrm function is built into an object file (.OBJ) to be used by programs written in compiled languages (C or PASCAL), or a dynamic library file (.DLL) to be used by programs written in interpreted or semicompiled languages (VISUAL BASIC, WINDEV) (col. 2., ll. 36-45). Steinmetz fails to disclose that the cnrm function – or any of the functions associated with the cnrm function – can be used within a structured query language (SQL) statement (emphasis added).

Moreover, in the Advisory Action of April 12, 2006, the Examiner states that "Steinmetz teaches using a structured language that contains at least two functions".

Even assuming, *arguendo*, that the Examiner is correct, Steinmetz fails to disclose utilizing at least two functions within a structured query language statement, as required by claim 1.

As the Applicant's specification explains, Relational DataBase Management System (RDBMS) software typically use a Structured Query Language (SQL) interface. The SQL interface has evolved into a standard language for RDBMS software and has been adopted as such by both the American National Standards Organization (ANSI) and the International Standards Organization (ISO) (specification, page 2, lines 2-6). Steinmetz fails in general to disclose utilizing SQL – or SQL statements – with respect to database management. Thus, Steinmetz cannot disclose utilizing at least two functions within a structured query language statement.

(B) Claims 21-23 and 25-27

Claim 21 recites a method for integrating encryption functionality into a database system. In particular, the method includes defining a function to support encryption of data in a database system, in which the encryption of data is based on a user-specified password, and the function has a function name. The method further includes utilizing the function within a structured query language, in which the structured query language statement includes the function name and the user-specified password.

Steinmetz fails to disclose utilizing a function (to support encryption of data) within a structured query language, in which the structured query language statement includes the function name and the user-specified password, as required by claim 23 (emphasis added). As discussed above, Steinmetz fails to disclose utilizing SQL – or SQL statements – with respect to database management. Consequently, Steinmetz cannot

disclose the additional detail of the structured query language statement including the function name and the user-specified password.

(C) The Examiner has not established anticipation under 35 U.S.C. §102.

Anticipation under 35 U.S.C. §102 requires the disclosure in a single piece of prior art of each and every limitation of a claimed invention. *Electro Med. Sys. S.A. v. Cooper Life Sciences*, 34 F.3d 1048, 32 USPQ2d 1017, 1019 (Fed. Cir. 1994). The Examiner has failed to show that the elements discussed in Sections (1)(A)-(1)(B) above are disclosed in Steimetz. Thus, claims 1 and 21 are improperly rejected under 35 U.S.C. §102(e) as being anticipated by Steimetz. Claims 2-5 depend from claim 1 and are, therefore, improperly rejected for at least the same reasons. Claims 22-23 depend from claim 21 and are improperly rejected for those reasons set forth with respect to claim 21.

Independent claims 8 and 15 each incorporates limitations similar to those of claim 1 and are, therefore, improperly rejected for at least the same reasons. Claims 9-12 and 16-18 respectively depend from claims 8 and 15, therefore, these claims are improperly rejected for at least the same reasons.

Independent claim 25 incorporates limitations similar to those of claim 21 and is, therefore, improperly rejected for at least the same reasons. Claims 26-27 depend from claim 25, therefore, these claims are improperly rejected for at least the same reasons.

2. Claims 6-7, 13-14, 19-20, 24 and 28 are not properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Steinmetz in view of Grawrock.

(A) Claims 6-7, 13-14, 19-20, 24, and 28

Claim 6-7 depends from claim 1, claims 13-14 depend from claim 8, claims 19-20 depend from claim 15, claim 24 depends from claim 21, and claim 28 depends from claim 25.

Grawrock discloses a method of securely and automatically authenticating a user. Putting aside the issue of whether Grawrock discloses the limitations of claims 6-7, 13-14, 19-20, 24 and 28, Grawrock (as with Steinmetz) fails to disclose utilizing SQL – or SQL statements – with respect to database management. Consequently, Grawrock fails to disclose utilizing at least two functions within a structured query language statement. Grawrock also fails to disclose utilizing a function (to support encryption of data) within a structured query language, in which the structured query language statement includes the function name and the user-specified password. Nor does the Examiner cite Grawrock as disclosing these limitations. The Applicant respectfully submits that claims 6-7, 13-14, 19-20, 24, and 28 are, therefore, improperly rejected for reasons similar to those discussed above.

(B) The Examiner has failed to establish a *prima facie* case of obviousness.

To establish a *prima facie* case of obviousness, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

As discussed above, both Steinmetz and Grawrock fail to disclose utilizing at least two functions within a structured query language statement. Steinmetz and Grawrock also fail to disclose utilizing a function (to support encryption of data) within a structured query language, in which the structured query language statement includes the function

name and the user-specified password. Consequently, the combination of Steimetz and Grawrock cannot render claims 6-7, 13-14, 19-20, 24, and 28 obvious.

Conclusion

Neither Steimetz nor Grawrock discloses utilizing at least two functions within a structured query language statement. Steimetz and Grawrock also fail to disclose utilizing a function (to support encryption of data) within a structured query language, in which the structured query language statement includes the function name and the user-specified password. The Applicant, therefore, respectfully submits that the pending claims 1-28 are not properly rejected under § 102 or § 103.

Please charge any fee that may be necessary for the continued pendency of this application to Deposit Account No. 09-0460 (IBM Corporation).

Respectfully submitted,
SAWYER LAW GROUP LLP

September 6, 2006

Date



Kelvin M. Vivian
Attorney for Applicant
Reg. No. 53,727
(650) 475-1448

Appendix of Claims

1. (Original) A method for integrating encryption functionality into a database system, the method comprising:
 - (a) providing at least two functions to support data encryption in a database system; and
 - (b) utilizing the at least two functions within structured query language statements.
2. (Original) The method of claim 1, wherein step (a) further comprises (a1) adding the at least two functions as user-defined functions in the database system.
3. (Previously Presented) The method of claim 2, wherein the user-defined functions further comprise a first function to encrypt user-specified data when inserted or updated in the database system.
4. (Original) The method of claim 3, wherein the user-defined functions further comprise a second function to decrypt the user-specified data when selected from the database system.
5. (Original) The method of claim 3, wherein the first function further encrypts the user-specified data with a user-specified password.

6. (Original) The method of claim 5, wherein the first function further encrypts with a password hint.

7. (Original) The method of claim 6, wherein the user-defined functions further comprise a third function to get the password hint.

8. (Previously Presented) A system for integrating encryption functionality into a database system, the system comprising:

at least one computer processing device; and

a database management system installed on the at least one computer processing device, the database management system supporting utilization of at least two functions for data encryption,

wherein the at least two functions for data encryption are invoked within structured query language statements.

9. (Original) The system of claim 8, wherein the at least two functions further comprise user-defined functions in the database management system.

10. (Previously Presented) The system of claim 9, wherein the user-defined functions further comprise a first function to encrypt user-specified data when inserted or updated in the database management system.

11. (Original) The method of claim 10, wherein the user-defined functions further comprise a second function to decrypt the user-specified data when selected from the database management system.
12. (Original) The system of claim 10, wherein the first function further encrypts the user-specified data with a user-specified password.
13. (Original) The system of claim 12, wherein the first function further encrypts with a password hint.
14. (Original) The system of claim 13, wherein the user-defined functions further comprise a third function to get the password hint.
15. (Original) A computer readable medium containing program instructions for integrating encryption functionality into a database system, the program instructions comprising:
 - (a) providing at least two functions to support data encryption in a database system; and
 - (b) utilizing the at least two functions within structured query language statements.

16. (Previously Presented) The computer readable medium of claim 15, wherein step (a) further comprises (a1) adding the at least two functions as user-defined functions in the database system.

17. (Previously Presented) The computer readable medium of claim 16, wherein the user-defined functions further comprise a first function to encrypt the user-specified data when inserted or updated in the database system, and a second function to decrypt the user-specified data when selected from the database system.

18. (Previously Presented) The computer readable medium of claim 17, wherein the first function further encrypts the user-specified data with a user-specified password.

19. (Previously Presented) The computer readable medium of claim 18, wherein the first function further encrypts with a password hint.

20. (Previously Presented) The computer readable medium of claim 19, wherein the user-defined functions further comprise a third function to get the password hint.

21. (Previously Presented) A method for integrating encryption functionality into a database system, the method comprising:

defining a function to support encryption of data in a database system, the encryption of data being based on a user-specified password, the function having a function name; and

utilizing the function within a structured query language statement to control access to the data in the database system including encrypting the data within the database system with the user-specified password,

wherein the structured query language statement includes the function name and the user-specified password.

22. (Previously Presented) The method of claim 21, wherein the function is a user-defined function or a built-in function within the database system.

23. (Previously Presented) The method of claim 21, wherein defining a function to support encryption comprises:

defining an encrypt function to encrypt data when inserted or updated in the database system; and

defining a decrypt function to decrypt data when selected from the database system.

24. (Previously Presented) The method of claim 23, wherein:

the encrypt function further encrypts a password hint that assists a user in remembering the user-specified password; and

the method further includes defining a third function to get the password hint.

25. (Previously Presented) A computer readable medium containing program instructions for integrating encryption functionality into a database system, the program instructions comprising:

defining a function to support encryption of data in a database system, the encryption of data being based on a user-specified password, the function having a function name; and

utilizing the function within a structured query language statement to control access to the data in the database system including encrypting the data within the database system with the user-specified password,

wherein the structured query language statement includes the function name and the user-specified password.

26. (Previously Presented) The computer readable medium of claim 25, wherein the function is a user-defined function or a built-in function within the database system.

27. (Previously Presented) The computer readable medium of claim 25, wherein defining a function to support encryption comprises:

defining an encrypt function to encrypt data when inserted or updated in the database system; and

defining a decrypt function to decrypt data when selected from the database system.

28. (Previously Presented) The computer readable medium of claim 27, wherein:

the encrypt function further encrypts a password hint that assists a user in remembering the user-specified password; and
the method further includes defining a third function to get the password hint.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None